EXHIBIT
1

MITRE

MP220250
MITRE PRODUCT

Independent Technical Review: *Security Analysis of Georgia's ImageCast X Ballot Marking Devices*

The analyses, views, opinions, and findings contained in this report are those of The MITRE Corporation only and should not be construed as those of any other person, organization, or company.

McLean, VA

July 2022

Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-1976

Executive Summary

Dominion Voting Systems Corp., via counsel Susman Godfrey, L.L.P., retained MITRE's National Election Security Lab (NESL) to provide an independent expert technical review of claims made by a researcher concerning the security of specific devices used in the conduct of elections in the State of Georgia. On behalf of the plaintiffs in *Curling v. Raffensperger*,[1] the researcher submitted a security analysis of Georgia's ImageCast X (ICX) Ballot Marking Devices (BMDs). These devices, produced by Dominion Voting Systems Corp., are currently distributed state-wide to every electoral precinct and have become the primary mechanism through which Georgia voters make selections and print ballots during elections. In the security analysis, the researcher claims to have exploited vulnerabilities in Georgia's BMDs that "could be effectuated by malicious actors with very limited time and access to the machines" and that it would be possible to commit "large-scale fraud" with "only moderate technical skills."

In this report, as an independent technical reviewer, MITRE NESL undertakes a technical analysis to assess the feasibility of the researcher's proposed attacks to change the outcome of a Georgia election. Without access to Georgia voting equipment or the researcher's proof-of-concept capabilities, MITRE NESL began by assuming validity of the researcher's technical capabilities. The researcher was provided with unrestricted physical access, system documentation, and passcodes for the devices examined. Under these conditions, security researchers may reasonably be assumed capable of compromising a device, regardless of manufacturer. MITRE NESL summarizes and assesses each of the researcher's principal findings, attack capability claims, and main conclusions.

MITRE NESL observed six total attack scenarios hypothesized by the researcher. Four of the proposed attacks involve replacing election software on BMDs with malicious software that alters a ballot before being printed and is disguised to look like Dominion's official application; one attack inserts malicious hardware components into a BMD printer; and one describes a ballot stuffing scenario.

The researcher's proposed attacks were assessed by MITRE NESL to be operationally infeasible given two parameters: the normal operating procedures of a voting precinct and associated officials, and scale considerations. Each of the attacks requires access and/or opportunity that remains unavailable in the operational environment. Five of six attacks were deemed non-scalable, impacting a statistically insignificant number of votes on a single device at a time. One attack was technically scalable but also was assessed to be infeasible due to access controls in place in operational election environments, access required to Dominion election software, and access required to Dominion election hardware.[2] Five of the proposed attacks involve modifications to a printed ballot's Quick Response (QR) code—a non-authoritative portion of a Georgia ballot—that can be detected through Risk-Limiting Audits (RLAs).

MITRE NESL has no evidence that any of the researcher's proposed attacks, in whole or in part, have been attempted by any party in an election.

[1] Dominion Voting Systems Corp. is not a party in the referenced litigation.

[2] MITRE's assessment of the researcher's proposed attacks assumes strict and effective controlled access to Dominion election hardware and software.